PLAN DE CLASE · Aegis8 Educa

Reconocer el Phishing

Los alumnos aprenden a identificar mensajes falsos, detectar señales y actuar correctamente.

Nivel: 7° básico – 2° medio **Duración: 60 min** **Formato: Grupal**

Objetivos

- → Definir qué es el phishing y por qué funciona psicológicamente.
- → Identificar al menos 5 señales de alerta en un mensaje sospechoso.
- → Aplicar una rutina de verificación antes de hacer clic.

Desarrollo de la clase

1. **Enganche — El costo de un clic**
   10 min
   Pregunta inicial: "¿Alguien conoce a alguien que haya caído en una estafa online?" Muestra 2 estadísticas: 22 millones de intentos de phishing en Chile 2024. Muestra un ejemplo de email de phishing real (anonimizado).
2. **¿Qué es el phishing?**
   10 min
   Phishing = imitar algo legítimo para robar datos. Tipos: SMS (smishing), WhatsApp, correo, llamada (vishing). El factor psicológico: urgencia, miedo, recompensa. La IA hace los correos perfectos.
3. **Análisis grupal de casos reales**
   20 min
   Grupos de 3-4. Cada grupo analiza 2 capturas reales de mensajes (el docente las imprime). ¿Es real o falso? ¿Por qué? ¿Qué señales ven? Puesta en común con todo el curso.
4. **Los 5 pasos de verificación**
   10 min
   El docente dicta los 5 pasos. Los alumnos los guardan en el teléfono o cuaderno. Demo opcional: Analizador de Phishing de Aegis8 (aegis8.org/analizador-phishing).
5. **Cierre y compromiso**
   10 min
   Cada alumno escribe 1 cosa que hará diferente esta semana. Tarea: enseñar los 5 pasos a alguien en casa — un familiar que pueda ser vulnerable.

Los 5 pasos de verificación

- Reviso quién manda el mensaje — ¿conozco este número/email?
- Busco errores de ortografía o redacción extraña (aunque hoy la IA los elimina)
- No hago clic en links — voy directamente al sitio oficial
- Nunca ingreso contraseñas desde un link recibido por mensaje
- Si tengo dudas, llamo directamente a la institución por su número oficial